



Document Summary

[Preview Claims](#)[Preview Full Text](#)[Preview Full Image](#)Email Link: **Document ID:** JP 09-269930 A2**Title:** METHOD AND DEVICE FOR PREVENTING VIRUS OF NETWORK SYSTEM**Assignee:** HITACHI LTD**Inventor:** KONDO TAKESHI
SHIGESA HIDEHIKO**US Class:****Int'l Class:** G06F 15/00 A; G06F 09/06 B; G06F 13/00 B**Issue Date:** 10/14/1997**Filing Date:** 04/03/1996**Abstract:**

PROBLEM TO BE SOLVED: To construct a computer network system whose resistance against a computer virus is strong.

SOLUTION: A frame repeater 100 has a means 202 for checking whether the computer virus is contained in a repeating frame or not and a warning message frame generation means 203 started at the time of detecting a virus frame. A means for receiving and displaying a warning message is provided in a computer connected to a network. Since the invasion of the computer virus, the diffusion and the influence range of damage can be set to minimum, the computer network system of high safety and reliability, which is provided with a resistance means for computer virus can be provided.

(C)1997,JPO

THIS PAGE BLANK (USPTO)

特開平9-269930

〈43〉公開日 平成9年(1997)10月14日

| (51) Int.Cl. ^a | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
|---------------------------|-------|--------|---------------|---------|
| G 0 6 F 15/00 | 3 3 0 | | G 0 6 F 15/00 | 3 3 0 A |
| 9/06 | 5 5 0 | | 9/06 | 5 5 0 Z |
| 13/00 | 3 5 1 | | 13/00 | 3 5 1 Z |

審査請求 未請求 請求項の数28 O L (全 23 頁)

(21) 出願番号 特願平8-81184
(22) 出願日 平成8年(1996)4月3日

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(72) 発明者 近藤 毅
神奈川県川崎市麻生区王御寺1099番地株式会社日立製作所システム開発研究所内
(72) 発明者 重左 秀彦
神奈川県海老名市下今泉810番地株式会社日立製作所オフィスシステム事業部内
(74) 代理人 弁理士 小川 勝男

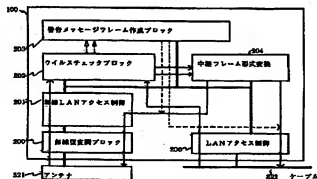
(54) 【発明の名称】 ネットワークシステムの防疫方法及びその装置

(57) 【要約】

【課題】 コンピュータウイルスへの耐性が高いコンピュータネットワークシステムを構築する。

【解決手段】 フレーム中継装置100に中継フレームにコンピュータウイルスが含まれていないかどうかをチェックする手段202とウイルスフレーム検出時に起動される警告メッセージフレーム作成手段203とを備える。前記警告メッセージを受信し表示する手段をネットワークに接続されたコンピュータに設ける。コンピュータウイルスの侵入やその拡散及びその被害の影響範囲を最小限にすることができるのでコンピュータウイルスへの対抗手段を備えた安全性および信頼性の高いコンピュータネットワークシステムを提供できる。

図 2



【特許請求の範囲】

【請求項 1】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、当該ウイルスチェックステップにおいて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリングステップと、前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報ステップと、当該警告通報ステップによる警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示ステップと、前記ウイルスのフィルタリングステップにより阻止された前記データが受信先に到達しないことによる影響を処理する後処理ステップとを有することを特徴とするネットワークシステムの防疫方法。

【請求項 2】ウイルスチェックステップで、データ圧縮または暗号の少なくとも一方により変形したコンピュータウイルスを識別することを特徴とする請求項 1 記載のネットワークシステムの防疫方法。

【請求項 3】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出したことにより、当該データに関連するコンピュータに警告メッセージを送信する警告通報ステップと、前記警告通報ステップにより送られた前記警告メッセージを受信したことを契機に、検出されたウイルスに対抗する処理を実行するウイルス駆除ステップとを有することを特徴とするネットワークシステムの防疫方法。

【請求項 4】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定ステップと、前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報ステップと、前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼ステップと前記検査依頼を受けて検査を実行

する検査ステップと前記検査ステップにおける検査結果を依頼者に報告する報告ステップとを有することを特徴とするネットワークシステムの防疫方法。

【請求項 5】コンピュータネットワークシステムは、複数の異なる伝送路と、当該伝送路を中継する中継装置を備え、

検査ステップにおける検査でコンピュータウイルスが入っているとしてたデータファイルから当該コンピュータウイルスの識別情報を抽出するステップと、

10 当該識別情報を前記中継装置に配布するステップと、前記中継装置において、前記ステップにより送られたウイルス識別情報を登録し、これに基づいてウイルスフィルタリングを実行するステップとを有したことを特徴とする請求項 4 記載のネットワークシステムの防疫方法。

【請求項 6】中継装置は、新規ウイルス識別情報を定期的に隣接するネットワーク中継装置と交換する機能を備えたことを特徴とする請求項 5 記載のネットワークシステムの防疫方法。

【請求項 7】伝送路に当該伝送路上のデータをモニタする監視装置を接続し、検査ステップにおける検査でコンピュータウイルスが入っているとしてたデータファイルから当該コンピュータウイルスの識別情報を抽出するステップと、

当該識別情報を前記監視装置に配布するステップと、前記監視装置において、前記ステップにより送られたウイルス識別情報を登録し、これに基づいてウイルスチェックを実行するステップとを有したことを特徴とする請求項 4 記載のネットワークシステムの防疫方法。

【請求項 8】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、

当該ウイルスチェック手段にて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリング手段と、

前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報手段と、

40 当該警告通報手段からの警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示手段と、

前記ウイルスのフィルタリング手段により阻止された前記データが受信先に到達しないことによる影響を処理する後処理手段とを具備して成るネットワークシステムの防疫装置。

【請求項 9】コンピュータネットワークシステムは複数の異なる伝送路と、当該伝送路を中継する中継装置を備え、当該中継装置に、ウイルスチェック手段とフィルタ

3

リング手段を具備し、前記中継装置のフィルタリング手段はウイルスが含まれたデータを中継しないことによりデータの伝送路上の通過を阻止する請求項8記載のネットワークシステムの防疫装置。

【請求項10】コンピュータは、当該コンピュータ上で動作するネットワークを使用したアプリケーションプログラムが異常終了したとき、ネットワークの故障によるものか、あるいはウイルス侵入防止によるものかをきり分ける手段を備えたことを特徴とする請求項8記載のネットワークシステムの防疫装置。

【請求項11】中継装置は、特定の情報を制御ヘッダに付加した伝送フレームをウイルスチェック結果にかかわらず中継することを特徴とする請求項9記載のネットワークシステムの防疫装置。

【請求項12】ウイルスチェック手段は、データ圧縮ないしは暗号により変形したコンピュータウイルスを識別する手段を備えて成る請求項8記載のネットワークシステムの防疫装置。

【請求項13】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、

前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出したら、当該データに関連するコンピュータに警告メッセージを送信する警告通報手段と、前記警告通報手段から送られた前記警告メッセージを受信したことを契機に検出されたウイルスに対抗する処理を実行するウイルス駆除手段とを有することを特徴とするネットワークシステムの防疫装置。

【請求項14】伝送路に、当該伝送路上のデータをモニタする監視装置を接続し、当該監視装置にウイルスチェック手段と、警告通報手段とを備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項15】コンピュータは、警告通報手段からの警報メッセージを受信する手段と、当該メッセージに基づき当該コンピュータのユーザにウイルス侵入警告を表示する手段とを備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項16】監視装置は、ワクンプログラムを格納する手段と、検出されたウイルスに対応するワクンプログラムに関連するコンピュータに送付する手段とを備えたことを特徴とする請求項14記載のネットワークシステムの防疫装置。

【請求項17】伝送路に、限定された範囲のネットワークをモニタするネットワーク監視装置を複数接続し、複数のモバイルコンピュータも接続したネットワークシステムにおいて、予め定めた特定範囲に所在する前記ネットワーク監視装置にウイルス検出メッセージを配布する手段を備えたことを特徴とする請求項13記載のネッ

4

トワークシステムの防疫装置。

【請求項18】無線ネットワークに接続する複数のモバイルコンピュータをネットワークシステムの構成要素として含み、当該モバイルコンピュータでのウイルス警告メッセージの表示において、検出されたウイルスに対応するワクンプログラムの実行が完了するまで電源を切らないことと、他のセルに移動しないようにとの注意事項をユーザに通知する手段を備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

10 【請求項19】コンピュータに、ウイルスチェック手段と、警告通報手段とを備え、更に警告メッセージからウイルスを送り出したコンピュータの識別情報を認識してこれを記憶する記憶手段と、前記記憶手段に登録されたコンピュータとの通信を控えさせる手段と、前記記憶手段に登録されたウイルス保有コンピュータのウイルス駆除完了通知により前記記憶手段から当該コンピュータを削除する手段とを備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項20】コンピュータは、モバイルコンピュータであり、ウイルスを送信したコンピュータの位置情報を警告メッセージから認識する手段と、ウイルスを保有したコンピュータの所在を提示する手段とを備えたことを特徴とする請求項19記載のネットワークシステムの防疫装置。

【請求項21】ウイルス送信コンピュータの登録手段と、ウイルス送信コンピュータ登録の解除手段と、前記手段により登録を解除されたことを通報する手段とを備えたことを特徴とする請求項14記載のネットワークシステムの防疫装置。

30 【請求項22】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定手段と、前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報手段と、前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼手段と、

40 前記検査依頼を受けて検査を実行する検査手段と、前記検査ステップにおける検査結果を依頼者に報告する報告手段とを有することを特徴とするネットワークシステムの防疫装置。

【請求項23】ウイルス推定手段にて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリング手段を備えて成る請求項22記載のネットワークシステムの防疫装置。

【請求項24】検査依頼手段による検査依頼中のデータファイルのアクセスを禁止する手段を備えたことを特徴

50

とする請求項2記載のネットワークシステムの防疫装置。

【請求項25】他のコンピュータからの検査依頼受付機能と、当該コンピュータに対する前記検査結果を報告する機能とを備えたことを特徴とする請求項22記載のネットワークシステムの防疫装置。

【請求項26】伝送路に当該伝送路上のデータをモニタする監視装置を接続し、コンピュータに新規ウイルスにたいするワクチンプログラムの作成手段を備え、前記監視装置に対して、前記新規ウイルスに対するワクチンプログラムを配布する手段を備えたことを特徴とする請求項22記載のネットワークシステムの防疫装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータネットワークシステムの安全性を高める発明であり、特に安全性を保証しにくいモバイルコンピュータを接続した無線ネットワークから、安全性や信頼性要求される基幹ネットワークにコンピュータウイルスやコンピュータワームが進入することで、基幹ネットワーク上のコンピュータにシステムダウン等の悪影響を与える事を抑止する発明である。

【0002】また、たとえ、当該ネットワーク上のコンピュータがウイルスに感染したとしても、そこからウイルス感染を拡大させないことで、コンピュータウイルスによって被害をうけるコンピュータをなるべく少なく抑えるコンピュータネットワークシステムに関する発明でもある。

【0003】また、ウイルスにより汚染されたコンピュータにたいしてウイルスワクチンソフトをすばやく汚染コンピュータに投与実施することによりウイルスをすばやく駆除することにより、ウイルスにたいする耐性を強化したコンピュータネットワークシステムに関する発明でもある。

【0004】

【従来の技術】パーソナルコンピュータをパソコン通信用のネットワークやインターネットに接続し、それらのネットワークのサーバに格納されたファイルをダウンロードすることが広く普及している。前述したファイルにコンピュータウイルスが潜んでいるとそのファイルの実行時等に当該コンピュータ内に寄生する。寄生したコンピュータウイルスは、潜伏したり、再感染のための自己複製を作る。そして、コンピュータウイルスは、ある条件が整うとソフトウェアを破壊するなどの様々な悪影響を与える。これを除去するためにコンピュータウイルスのワクチンソフトを定期的に起動して感染していないかチェックすることで、コンピュータウイルスを除去している。

【0005】特に、インターネットでは、情報提供者としてのビジネスの利用や各種の情報を入手できるメリッ

ト等があるため、企業において、従来の企業内ネットワークをインターネット接続する例が増えている。このような企業内ネットワークでは、信頼性が必要であり、パスワードによる認証等により、各種ネットワーク機器へのアクセスを監視することで信頼性を保っていた。例えば、このような技術に関する発明が「ローカルエリアネットワークのセキュリティ方法及びそのシステム」として特開平7-131451で公開されている。

【0006】セキュリティを保ちながら、インターネット接続する方法として、ファイアウォール等でアクセス者を限定する方法があるが、コンピュータウイルスにたいする対策は、上述したように、個々の計算機で上述した方法で対応しており、システム的な対応はなされていない。

【0007】また、多数のコンピュータが接続するインターネットは、セキュリティに関しては非常に低いレベルにある。このため、悪意あるハッカー達により、今までにない新しいコンピュータウイルスが開発され、これが流行する恐れもある。それは、このような新しいウイルスに対応したワクチンが開発される迄時間がかかることもしこのような新しいウイルスの潜伏期間が長いと新しいウイルスの検出までに時間がかかることによる。このような新しいコンピュータウイルスに対抗するため、あるコンピュータでウイルスによる異常を監視しておき、異常を検出したらそのウイルスの識別子を特定し、その特定情報を各コンピュータに配布するという方法が「コンピュータを生態免疫システムの強化する方法」としてJeffrey O. Kephartが「To appear in Artificial Life IV, R. Brooks and P. Mea s. eds., MIT Press, 1994で発表している。

【0008】

【発明が解決しようとする課題】上記従来技術によると、以下のような課題がある。

【0009】課題1：ウイルスが当該マシンに侵入したとき、ウイルススキャンプログラムやワクチンプログラムを起動するまでの間にネットワークを介して他のマシンに二次感染する。即ち、ウイルスの蔓延を防ぐ事ができない。

【0010】課題2：例えばファイルをダウンロードするたびにウイルスチェックのためスキャンプログラムやワクチンプログラムを起動したのでは、マシンにオーバヘッドがかかる。また、ファイルの起動のたびに前記プログラムをいちいち起動するのは、ユーザにとって煩わしい作業である。

【0011】課題3：また、いつワクチンを起動すれば適切かわからないため、通常、定期的にウイルスチェックプログラムを実行する。このような場合、ウイルスに感染していきなくて、ウイルスチェックプログラムによるメモリチェック等の処理負荷がコンピュータにかかる。

【0012】課題4：更に、悪意を持った者がウイルスをばらまくために、ウイルス入りのファイルをだれでもアクセスできるサーバにアップロードするということも防げない。

【0013】等である。

【0014】

【課題を解決するための手段】上記課題は、以下の次の手段、すなわち、

手段1：ウイルスフィルタ機能を備えたネットワーク上を流れるデータの中継手段または、

手段2：ウイルス検出メッセージ発信機能を備えた中継装置と前記メッセージを表示する機能を備えたコンピュータ装置

のいずれかによって原理的に解決できる。
【0015】すなわち、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、当該ウイルスチェックステップにおいて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリングステップと、前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報ステップと、当該警告通報ステップによる警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示ステップと、前記ウイルスのフィルタリングステップにより阻止された前記データが受信先に到達しないことによる影響を処理する後処理ステップとを有することにある。

【0016】また、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出したことにより、当該データに関連するコンピュータに警告メッセージを送信する警告通報ステップと、前記警告通報ステップにより送られた前記警告メッセージを受信したことを契機に、検出されたウイルスに対抗する処理を実行するウイルス駆除ステップとを有することにある。

【0017】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定ステップと、前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場

合、注意メッセージを前記データの受信コンピュータに送付する注意通報ステップと、前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼ステップと、前記検査依頼を受けて検査を実行する検査ステップと、前記検査ステップにおける検査結果を依頼者に報告する報告ステップとを有することにある。

【0018】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、当該ウイルスチェック手段にて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリング手段と、前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報手段と、当該警告通報手段からの警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示手段と、前記ウイルスのフィルタリング手段により阻止された前記データが受信先に到達しないことによる影響を処理する後処理手段とを具備して成るネットワークシステムの防疫装置にある。

【0019】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出したら、当該データ関連するコンピュータに警告メッセージを送信する警告通報手段と、前記警告通報手段から送られた前記警告メッセージを受信したことを契機に検出されたウイルスに対抗する処理を実行するウイルス駆除手段とを有することにある。

【0020】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定手段と、前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報手段と、前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼手段と、前記検査依頼を受けて検査を実行する検査手段と、前記検査ステップにおける検査結果を依頼者に報告する報告手段とを有することにある。

【0021】上記のように構成すれば、ネットワーク上のコンピュータは、他のコンピュータとデータ通信することで、データファイルを自分のコンピュータのメモリ上にロードする。このようなネットワーク上でコンピュータは、ウイルス入りのファイルを検査し、これを実行したりするとウイルスに感染する。いま、中継装置を介して相互に接続するネットワークを考えれば、前述した手段1がウイルス入りのデータをフィルタするので、ウイルス入りのファイル等をリモートからアクセスしようとする、必ず当該ファイルのデータ通信が失敗する事になる。結果として、ウイルスに汚染されたファイルはアクセスできなくなるので、ウイルスに感染する事はなくなる。よって、ワクチンソフトを定期的に起動しなくともすむ。また、悪意を持ったユーザが、ウイルスをばらまこうとして、ウイルスの感染媒体であるファイルに、自由にアクセスできる公開されたファイルサーバに登録しようとしても、前記手段1によって、結果的にファイル転送が失敗する。これにより、ウイルス入りのファイルは当該ネットワークにおいて感染媒体としての役割を果たさなくなるため、ウイルスの拡散を防げる。

【0022】また、手段2によれば、ウイルス検出メッセージを受信したコンピュータは、ウイルス入りのファイルをロードしようとした事がわかるため、その対応をなすことができる。例えば、ウイルスに寄生される前なら当該ファイルを削除したりできる。また、ワクチンプログラムを当該メッセージ受信のタイミングで実行する事ができ、その結果ウイルスの駆除が直ちに行える。

【0023】

【発明の実施の形態】

実施例1

無線ネットワークから基幹ネットに接続されたコンピュータに侵入を企てているウイルスをネットワーク上の検知して、それをファイリングし侵入ターゲットとなつたコンピュータシステムにたいして、警告を与えるネットワークシステムの実施例をこれから説明する。

【0024】図1は、本発明の一実施例におけるシステム構成を表した図である。

【0025】本システムは伝送路に光や電波などの電磁波を使用した無線ネットワークと伝送路にケーブルを使用した有線ネットワークとを接続したコンピュータネットワークシステムであり、以下に述べるコンポーネントから構成される。100は、無線ブリッジ（以下WBと略称する）であり、有線ネットワークと無線ネットワークとの接続装置である。無線ブリッジ100は、有線ネットワークを流れるデータフレームを無線ネットワーク側に中継したり、またその逆に無線ネットワーク上を流れるデータフレームを有線ネットワーク上に中継したりする。

【0026】101は、個人用の計算機システムである

パーソナルコンピュータ（以下PCと略称する）である。PC101は、有線ネットワーク上に接続され、ネットワークに接続された他の計算機システムとデータ通信を行う。

【0027】102は、ポータブルな計算機システムであるモバイルコンピュータ（以下MTと略称する）である。MT102は、無線受信機を使用して無線ネットワークに接続し、ネットワークに接続された他の計算機システムとデータ通信を行う。例えば、PC101に電子メールや電子化されたファイルを蓄積しておき、MT102を離れた場所に持ち込み、その場で前述の電子メールを読んだり、電子ファイルの内容を更新したりする。

【0028】103は、有線ネットワーク上を流れるデータの配送を制御するルータである。ルータ103は、複数のネットワークと接続し、パケット化されたデータ（単にパケットと呼ぶ）に記された配送アドレスに応じて、あるネットワーク上のパケットを他のネットワークに送る機能を持つ。

【0029】104は、WB100の無線機がカバーするエリアである無線LANセルである。本セル内では、同一の周波数帯域が使用されるため、当該セル内に収容されているMT102間で通信ができる。

【0030】105は、ローカルエリアネットワーク（以下LANと略称する）であり、先述したPC101やWB100、MT102が複数台接続したルータ103によって仕切られた局地的なネットワークである。このローカルネットワーク105は、MT102とWB100から構成される無線LANを含んでいる。

【0031】106は、インターネットであり、前述したルータ103により相互接続されたコンピュータネットワークの集合体である。

【0032】まず、本発明のネットワーク防疫機能をWB100に実装した例を説明する。

【0033】図2で示すWB100内の各機能ブロックによってMT102からPC101へのウイルス進入防止機構が実現される。

【0034】WB100は、先述したように、有線ネットワーク上でデータフレームを無線ネットワーク上に中継したり、またその逆方向の中継も行う。そのための機能ブロックが無線復調ブロック200、無線LANアクセス制御201、中継フレーム変換204、及びLANアクセス制御205の各ブロックである。これらのフレーム中継機能ブロックに対して、ウイルスの進入をフィルタすることによりネットワークの安全性を高める機能ブロックが、ウイルスチェックブロック202と警告メッセージフレーム作成ブロック203である。無線ネットワーク側から基幹ネットワークである有線ネットワーク側へ侵入しようとするコンピュータウイルスを例にして各ブロックの働きを説明する。

11

【0035】まずアンテナ321でデータフレームの情報
 が乗せられた電波を受け取る。そして、無線復調ブ
 ロック200が受信電波信号からフレームを構成する信
 号を取り出し、そこから無線LANアクセス制御201
 がデータフレームを再構築する。次に、受信したデータ
 フレームの中に、コンピュータウイルスを構築するた
 めの情報が入っていないかどうかをウイルスチェックブ
 ロックが検査する。この結果、ウイルスを含まないフ
 レームならば、次のブロックである中継フレーム形式変換2
 04に送られる。中継フレーム形式変換204は、無線
 側と有線側のフレーム形式の変換する。そして、有線L
 AN上のフレームに変換された後、LANアクセス制御
 205に渡り、そこから有線ケーブル322上にフレー
 ム信号が送出される。これに対して、ウイルスチェッ
 クブロック202で、ウイルスが含まれていると判定され
 たフレームは、中継フレーム変換204に渡さない
 ので、有線ネットワーク側に流れず、WB100ないで阻
 止される。このときウイルスチェックブロック202
 は、警告メッセージフレーム作成ブロック203に受信
 フレームでウイルスを検出した事を通知する。これを受け
 20 った警告メッセージ作成ブロック203は、ウイルス検
 出警告メッセージを作成し、ウイルス入りフレームの送
 り元とその宛先にたいして、前記メッセージを送るた
 め、それぞれ、無線LANアクセス制御201とLAN
 アクセス制御205に警告メッセージを渡す。これを受け
 けた各々の制御ブロックは、警告メッセージフレームを
 ネットワーク上に送出する。

【0036】次にWB100のハードウェア構造を図3
 を使って説明する。

【0037】300は、MPUでありWB100の処理
 ソフトウェアの実行ユニットである。RAM301は、
 MPU300が書き換え可能な記憶装置である。ROM
 302は、書き換え不可能な読みだし専用の記憶ユニ
 ャットであり、WB100の処理ソフトウェアが記憶されて
 いる。303は、LANの標準規格であるEthernetの
 制御LSIであり、伝送ケーブル322で接続される有
 線LANへのフレーム送信や有線LANからのフレーム
 受信を処理するハードウェアユニットである。310
 は、MPUバスであり、RAM301やROM302等
 の記憶装置や303、304等の出力制御LSIが接
 続されている。304は、無線LAN側の入出力制御LSI
 であり、バス310のインタフェース機能と無線L
 ANに対するアクセス制御を行う機能を備える。306
 は、復調LSIで有り、フレームを構成する情報を
 搬送電波に乗せるための信号に変調したり、逆に、搬送
 電波に乗せられた信号からフレームを構成する情報を取
 り出す復調したりする機能を持つ。306は、RFイン
 タフェースLSIであり、RFユニット307の発信・
 受信等の制御を行う。307は、RFユニットであり、
 使用帯域周波数の電波を送信したり、受信したりするユ
 50

12

ニットである。321はアンテナである。

【0038】次に、図4を用いてWB100の処理ソフ
 トウェアモジュール構成について説明する。

【0039】404は、無線LANドライバモジュール
 であり、無線LANのアクセス制御LSIである307
 の制御用ソフトウェアである。これに対して、406
 は、Ethernetドライバであり、Ethernet制御LSI
 303用の制御用ソフトウェアである。403は、LAN
 ドライバ共通制御で有り、無線LANと有線LANの
 10 制御においてフレーム送受信等の共通となる制御ロジッ
 クをまとめたソフトウェアモジュールである。402
 は、ブリッジ処理であり、フレーム形式の相互変換機能
 とフレーム中継機能、及び、フレームヘッダに配載され
 たアドレスによるフィルタリング機能を実現する。40
 1は、ウイルスチェックモジュールであり、ブリッジ処
 理における中継フレームの情報フィールドを見て、そ
 こにウイルスのコードが記載されていないかどうかをチェ
 ックし、ウイルス入りのフレームをフィルタリングする
 機能をもつ。400は、セキュリティ管理モジュールで
 あり、ウイルスフレームを検出した401から通知を受け
 けた後、当該フレームの送り元と宛先のアドレスに対
 する警告メッセージを作成する機能をもつ。405は、通
 信プロトコル処理モジュールであり警告メッセージを受け
 取るPC101やMT102上のセキュリティ管理プ
 ロセスに対するメッセージの配送を保証する機能を持
 つ。

【0040】次に、図4で示した各処理ソフトウェアモ
 ジュールがどのような処理ロジックによって総括されて
 いるかを図5のWB処理フローで説明する。まずはじめ
 のステップは、受信フレーム待ちであり(ステップ50
 2)、無線・有線LANの各ドライバ404、406か
 らドライバ共通制御403を介して正当なフレーム受信
 の報告が対応するハードウェアユニットからブリッジ処
 理402にいくまで待つステップである。次に、ブリ
 ジ処理部でのフィルタリングを行った後、ウイルスス
 チェックモジュール401で受信フレームの検査を行う
 (ステップ504)。ステップ504でのチェックで当
 該フレームにウイルスが含まれていなければ、中継処理
 ステップ510に移り、もし、含まれているならば、警
 告メッセージ作成ステップ506に移る。ウイルスが含
 まれていた場合のフローから説明する。

【0041】警告メッセージ作成ステップ506では、
 セキュリティ管理モジュール400で、送り元と宛先に
 に対する警告メッセージをウイルスチェック結果に応じて
 それぞれ作成するステップである。次は、メッセー
 ジフレーム処理ステップであり、前記メッセージに通信プロ
 トコルヘッダを付加してフレームを作成し、それぞれに
 2 に対するフレーム送信要求をLANドライバ共通制御40
 2に発行することを通信プロトコル処理405において
 実行する(ステップ508)。次にステップ502にお

13

いて当該フレームにウイルスを検出なかった場合の処理フローについて説明する。このときは中継処理ステップとしてブリッジ処理モジュール402でフレームの変換をしてLANドライバ共通制御403に異なるサイドLANに送出するように送信要求を出す(ステップ510)。残りの処理ステップは、フレーム送信であり、要求されたフレームを指定された側のLANに送出する処理を行い、はじめのステップ502に飛ぶ(ステップ512)。

【0042】次に、前述した警告メッセージ作成ステップ506で作成する警告メッセージの内容とそのWB100とPC101やMT102間の警告メッセージ通信プロトコルについて図6を用いて説明する。

【0043】図6(a)でプロトコルシーケンスについて説明する。本プロトコルは最も単純なプロトコルであり、WB100から警告メッセージ600のインディケーションで通知するプロトコルであり、PCからの問い合わせ等は行わないプロトコルである。したがって、送信側はメッセージを送るだけでプロトコル処理を終了する。これに対して受信側では、常にメッセージを受信できるように状態で待機している。これから、警告メッセージ600の内容について図6(b)を用いて詳述する。警告メッセージ600は、プロトコルID601、長さ602、警告内容603、フィルタードフレーム604の各フィールドから構成される。プロトコルID601は、本メッセージの正当性をチェックするための特定の識別情報が記載される。長さ602は、警告内容603の長さを示す。警告内容603は、どのMB100で何時、どのようなウイルスが検出されたかを示す情報が記載される。フィルタードフレーム604には、ウイルスが検出されたフレーム自身がききいされる。これによりウイルスフレームは本警告メッセージにラッピングされて送られる。

【0044】さて、次にPC100のハードウェア構成について図9を用いて説明する。

【0045】900は、CPUであり、本装置の中核を成すプログラムの処理装置である。CPU900は、CPUバス910を介して記憶装置であるRAM301やROM302らとI/O制御装置であるEterNet制御303やSCSI制御905や画面制御908らとインタフェースしている。また、このバスのインタフェース制御はバス制御904が制御する。SCSI制御905の先には、大容量の記憶装置であるハードディスク装置(hdと略称)906やCD-ROM装置(CDRと略称)907が接続される。また画面制御908の先には表示装置であるDISPLAY909が接続する。

【0046】次に、MT102のハードウェア構成も同様であるが、303の代わりに図3の304、305、306、307の無線LAN用の制御装置が付き、アンテナ321に接続される点が異なっている。

14

【0047】次に、PC101のソフトウェア構成について図8を用いて説明する。

【0048】800aは、ネットワークを使用して他のOC101やMT102等の計算機と通信する電子メール等の各種アプリケーションプログラム(APと略称)である。804は、OSカーネルであり本計算機の種々のリソース(メモリ、プロセス、I/O)を制御するプログラムである。803はLANドライバであり、LANとのデータのアクセスを制御する。802は、通信プロトコル処理でありネットワーク上のデータ転送を保証するプログラムである。801は、セキュリティ管理プログラムであり、WB100からの警告メッセージを受け取り、ユーザにたいして警告を通知するプログラムである。

【0049】つぎにこのセキュリティ管理プログラム801の処理フローについて図7を使用して説明する。

【0050】まず最初のステップは、メッセージ受信待ちステップ(ステップ700)である。メッセージを受信したら次のステップを実行する。次は、当該APの検出ステップである。これは、受信メッセージに記述された内容からウイルス入りのフレームを受信しようとしたAPを特定する(ステップ702)。次に当該APがコネクションをはっているならば、これを切断する(ステップ704)。次に当該APが閉じたままにしていたファイルがあればこれをクローズする(ステップ706)。次に当該プロセスを強制終了する(ステップ708)。次にウイルス入りのデータを受け取るうとして強制終了した事をユーザに伝えるためレポートを作成したのちこれを画面に出力する(ステップ708)。

【0051】MT102でもソフトウェア構成は、PC101と同様なので詳細を省略する。

【0052】次に、ウィンドによるGUI(グラフィカルユーザインタフェース)を備えたPCにおけるステップ708で画面に出力されるレポートについて図10を用いて説明する。

【0053】1001は、セキュリティ管理メッセージウィンドであり、当該APの強制終了とともに本ウィンドが生成される。1002は、1001内に表示されるレポートの内容である。これは、以下の各情報を出力表示する。AP名称として、強制終了されたAPの実行ファイル名。APログとして当該APが起動された時刻と強制終了された時刻、AP情報として通信相手に関する情報(ネットワークアドレス等)や強制クローズされたファイル名称等を表示する。1003は、本ウィンド制御ボタンであり、これが選択されると本ウィンド1001が閉じられる。1004は、他のAPの実行ウィンドである。

【0054】MT102におけるレポート出力も同様である。ただその内容がウイルス情報をネットワークに流そうとした事を警告するものであることが受信側のPC

と異なる点である。

【0055】次に、ウイルスチェックモジュール401とステップ504のウイルスフレームチェック処理ステップの詳細について図12, 11を用いて説明する。

【0056】図12における120は、ウイルスコードシグネチャリストであり、ウイルスの名称と当該ウイルスを識別するための特徴であるウイルスのコードの並びとから構成されている。

【0057】ネットワーク上を流れるフレームのデータは、圧縮されていたり、暗号化されている場合もある。このときは、シグネチャリストに記されたウイルスコードの圧縮後のビット列や暗号化後のビット列をシグネチャとして登録しておく。

【0058】図11のステップ1100は、上記リスト120の第一コラムのコードを取り出し、検査対象のフレーム内容を先頭から順次ウイルスコードと比較し一致していないかチェックする(ステップ1100)。一致していれば図5で示したステップ508に進む。次は、終了判定ステップである。検査フレームの最後に達してかつリスト120の最終コラムに記されたウイルスコードの比較が終了したかどうかを調べる(ステップ1102)。その結果終了したならばステップ510に飛ぶ。そうでなければ、リスト120の次のコラムのウイルスコードを比較のための内容として取り出す(ステップ1104)。次に最初のステップ1100から繰り返す。

【0059】このようにして、ネットワークのフレームに含まれるコンピュータウイルスを検出し、当該計算機(送り側と受け側双方)にたいして注意を促す事ができる。

【0060】実施例2

上記例では、警告メッセージ600にウイルスコードを含むフレームを包みこんで相手に渡していたが、例えば、悪意のあるユーザが本警告メッセージ600をネットワークから盗み見て既知のウイルスコードを入手し、新しいウイルスを開発しようとする事が有り得る。これを防止することで、より安全性を高めることができる。このために、ウイルスコードを含む警告メッセージを暗号化の手法により分からなくしておく。または、警告メッセージ600にはウイルスコードを付加せず、警告内容603にウイルスが検出されたフレームのヘッダ情報のみを付加する方法でもよい。

【0061】また、一般のユーザにたいしては、ウイルスフレームをシャットアウトし、ネットワークのセキュリティ管理者(検出ウイルスの解析やワクチン作成のために当該ウイルスを必要とする人)にたいしてのみ、ウイルスコードを含むフレームを前記カプセル化手法を用いて渡すようにしてもよい。このとき、ウイルスフィルタ機能を備えたWB100等の中継装置において、ネットワークセキュリティ管理者あるいはカプセル化されたウイルス入りフレームをきちんと中継するためには、セキ

ュリティ管理社宛のフレームについては、ウイルスフィルタをしない事が必要である。このためには、ウイルスフィルタ機能を備えた中継装置にセキュリティ管理者アドレスを登録しておく。そして図5で説明するとウイルスフレームチェック処理(ステップ504)の前に、フレームの宛先アドレスをチェックする処理ステップを追加し、登録された前記アドレス宛であればステップ504を実行しないで中継処理ステップ510に飛ぶことにより変更した処理ロジックで実現される。

【0062】実施例3

上記実施例では、無線LANと有線LANとの仲介装置である無線ブリッジであるWB100にウイルスフィルタ機能を備えた例で説明したが、本発明の方法は、LANとLANとの連結装置であるルータ103上においてもWB100で説明したのと同様な方法でウイルスフィルタ機能を容易に実現できる。

【0063】さて、以上では無線側から有線側へ進入することを防ぐ場合のシステムの構成や処理装置について述べてきた。逆の場合、即ち、有線側から無線側にウイルスが出ていくケースのウイルスフィルタ機能も前述した方法により実現できる。

【0064】実施例4

次は、同一セル104内に存在するMT102からMT102へウイルス入りのフレームが送られるケースでのウイルス侵入対策について図13を用いて述べる。本ケースでは、対等分散型の無線LANを想定しているため、WB100は、当該セル104の内を飛び交っているフレームをモニタできる。しかし、WB100は、セル内のMT102間通信でフレーム中継処理をしているわけでないで、実施例1で述べたようなウイルスフレームのフィードバックは実行できない。なお、集中方式の無線LANならば、WB100において中継処理を行っているため、実施例1と同様なウイルスフィルタリング機能をWB100で実現できる。

【0065】さて、対等分散型無線LANにおけるWB100では、無線フレームを常時モニタしている(ステップ1300)。ここで、ウイルス入りのフレーム131を発信したMT102があると、実施例1と同様な方法でウイルスフレームを検出する(ステップ1302)。その後警告メッセージをウイルスフレーム受信MT102宛に送り出す(ステップ1304)。しかし、これを受け取ったMT102は、実施例1で述べたPC101のケースと異なりウイルス入りのフレームを概に受信してしまっている。即ち、あるMT102がフレームの受信処理を実行している(ステップ1310)。ここで、ウイルスフレーム131が送られたとすると、その受信完了処理を実行してしまう(ステップ1312)。そのため、警告メッセージを受信する前には、MT102におけるウイルスフレームを受信したAPが既に終了している事も有り得る。例えば、ユーザ130が

17

MT102内に作成されたウイルス入りの実行ファイルをアクセスし(ステップ1330)、その結果システム内にウイルスが感染してしまっているケースも有り得る(ステップ1314)。その他、最悪のケースでは、さらに他のMT102へウイルスを感染させてしまった後のケースも有り得る。この後、警告メッセージを受けたMT102は、警告を表示する(ステップ1316)。したがって、ユーザ責任において、ウイルスに汚染された可能性のあるファイルをきり分けて削除するなり、ワクチンプログラム走らせて寄生しているかもしれないウイルスを退治する必要がある。もちろん、ここでは、ワクチンプログラムの起動等は、警告メッセージ表示と連携させて実行する。この場合は、WB100がウイルスのタイプを識別し、それに対応するワクチンソフトをメッセージ600の内容としてMT102に通知し(ステップ1306)、警告メッセージ600を受信したMT102は、警告メッセージ表示の後、ワクチンを受信し、受信したワクチンの実行確認をユーザにたいして求める(ステップ1318)。ユーザがワクチンソフトの起動を指示する(ステップ1332)。すると当該ワクチンソフトが実行される(ステップ1320)。こうしてウイルスが退治される。ここでは、ワクチンソフトは、MT102にストックして置く方式で説明したが、ワクチンをMT102がストックしておき、WB100からの警告メッセージにどのワクチンを使用すべきかを通知する方式でも、前記メッセージとともにワクチンを送付する方式でも実現できる。

【0066】先に述べた最悪のケースで二次感染した場合でも同様に、WB100が常時モニタしており、ウイルスフレーム発見時には、警告メッセージを受信MT102に送るのでウイルスへの対応がなされる。したがって、警告メッセージ受信前にMT102がパワーオフした他セルに移動したりして、メッセージを受信できないケースを除けば、当該セル内でウイルス感染は収束する。

【0067】実施例5

また、上記のウイルスフレーム受信MT102に対してのみ警告メッセージを送るのではなく、WB100がウイルスをモニタした時点で注意メッセージを当該セル内にブロードキャストし、セル内のすべてのMT102に対して注意を促してもよい。これによると二次感染する割合が減少し、すばやく感染がウイルス感染が収束する。

【0068】実施例6

これから、ウイルスを保有したMT102cがセル104間を移動するケースでの無線ネットワークシステムにおけるウイルス侵入対策の実施例を説明する。

【0069】ウイルスを保有したMT102cと通信するMT102bが同一セル104a内にあるとき、MT102bがウイルスフレーム受信前に他セル104bに

18

移動する場合は、WB100のウイルスフィルタ機能により対応される。そこで、ウイルス保有MT102cが他セル104bに移動するケースを例にして発明の詳細を説明する。

【0070】図14、15は、本実施例におけるWB100の警告メッセージ配布処理フローチャートであり、図14は、ウイルスフレーム検出後の警告メッセージ発行処理であり、図15は、他のWB100から警告メッセージを受信後のメッセージ配布処理である。

【0071】まず、WB100は、フレームをモニタし、そこにウイルスが入っていないか検査する(ステップ1400)。そして、ウイルスを検出したら次のステップを実行する。次は、フレームのヘッダからその送り元であるウイルス保有MTのアドレスを記憶する(ステップ1402)。次に、ウイルス保有MTには、ウイルス送出違反の警告メッセージを、ウイルスフレーム受信者には、ウイルスフレーム受信の警告メッセージを、そして、残る同一セル内のMT102に対してウイルスフレーム検出の警告メッセージを通知する(ステップ1404)。同一のLAN内の各WB100に対してマルチキャストでウイルス保有MT検出警告メッセージを通知。このとき、メッセージ中に参照カウントをセットしてメッセージを送り出す。また、各WBは、隣接する(ルータの先に接続した)LANにおける代表WBのアドレスを知っている。そして、ウイルスフレーム検出WBは、マルチキャスト範囲外の隣接するLANの代表WBに対して警告メッセージを通知(ステップ1406)。

【0072】次に図15にて、ステップ1406で発行された警告メッセージを受けたWBの処理を説明する。まず、警告メッセージを受信して、自分が代表WBであるかないかによって処理ケースを振り分ける(ステップ1500)。そして代表ならば、当該LAN内の他のWB100に配布するため警告メッセージをマルチキャストし、そして警告メッセージ中の参照カウントを減算して0かどうかをチェックする(ステップ1502)。そしてこの結果が、0ならば、これ以上隣接のWB100に配布しない、そうでなければ送り元を除く隣接する代表WBに対して警告メッセージを通知する(ステップ1504)。いづれかのケースでも最後は、受け持つセル内の全MTに警告メッセージを同報(ステップ1506)する。

【0073】なお、WBからWBへの警告メッセージの参照カウントは、検出されたウイルス保有MTの移動範囲が大きいものを程大きくして効果的に配布される。

【0074】上記警告メッセージにはウイルスMTを検出したWB100のアドレスが記述されており、ウイルスが検出されたセルの位置がわかるようになっている。上記警告を受け取った各WBにおいてウイルスが検出されたセルに近いものは、当該セル内の各MT102にウ

イルス保有MTを伝え、このMT102と通信するときには注意するように伝える。これにより、ウイルスに感染したMT移動してくることによるウイルスの感染に対して、前述の警告メッセージを受信したMT102は、必要に応じて備えることができる(当該MTと通信しない等)。また、最悪のケースとして、本警告メッセージ受信の前にウイルス保有MTが移動してきた場合には、各WB100でのウイルスフレーム検出・駆除機構に任せられる。また、警告メッセージを受けたMT102において、ウイルスが検出されたセルへ移動するものは、ウイルスのトラップを起動しておいてもよい。これにより、汚染セル(ウイルス駆除が完了していない)へ移動した場合での感染を防止する事ができる。

【0075】次に、図16を用いて警告メッセージを受け取るMTの処理フローを説明する。まず警告メッセージの振り分けを行う(ステップ1600)。ここで、ウイルスを検出したWB100のアドレスが現在のセルのWB100と一致していない場合は、異なるセルでウイルスが検出されたと判断して、ステップ1602から実行する。前記判定で、同一の場合はステップ1610から実行する。そして、また、自分がウイルス保有MTであるかを、警告メッセージから識別し、そうである場合はステップ1606から実行する。この処理の詳細では、後で述べる事とし、ここでは、それ以外のケース、即ち、自分がウイルス保有MTでない場合の処理について説明する。まず、他セルのケースから説明する。このケースでは、まず、ウイルス保有MTをウイルス保有者リスト250に登録する(ステップ1602)。

【0076】ここで、図25によりウイルス保有者リスト250について説明する。ウイルス保有者リスト250は、現在ウイルスを保有しているMTの識別情報を記憶したものであり、MTの識別情報が並んだ参照用のテーブルである。図16に戻り処理フローの続きを説明する。登録ステップ1602の後、注意メッセージをMT102の画面に表示する(ステップ1604)。次に、同一セルのケースを述べる。まず、ステップ1602と同様にウイルス保有者リストに登録する(ステップ1610)。次に、WB100から送られたワクチンプログラムの実行処理を行う(ステップ1612)。

【0077】先に説明したように、警告メッセージを受けたMT102は、ウイルスフレームを発信したMT102と通信する事は控える(原則として行わない)。これを果たする処理フローを図17で説明する。まず、起動されたAPが通信しようとしているかどうかをチェックする(ステップ1700)。ここで通信要求があれば次の処理を実行しそうでなければ繰り返す。次は、ウイルス保有者リストをチェックし、通信相手が登録されていないかを確認する(ステップ1702)。通信相手が登録されていれば、確信表示ステップ1704を

実行し、そうでなければ、通信処理(ステップ1714)を実行する。確信表示処理は、ユーザに対してウイルスを保有している相手との通信を望んでいるかを確認する処理ステップである。次にユーザからの応答を受け取りこれをチェックする(ステップ1706)。この結果ユーザが通信を希望する場合は、ステップ1708を実行し、そうでなければ、当該APを終了し(ステップ1710)、はじめのステップに戻る。ステップ1708は、通信相手へのウイルス駆除完了の問い合わせを実行し、その応答結果を判定する(ステップ1708)。この応答結果が、ウイルス駆除完了ならば、ウイルス保有者リストから通信相手MTを抹消し(ステップ1712)、通信処理ステップ1714を実行する。応答結果がウイルス駆除完了でなければ、当該APを終了して(ステップ1710)はじめてのステップ1700に戻る。

【0078】次に、ウイルス入りフレームを発信したMT102は、以後他のMT102と通信されなくなるため、これを解除する方法を説明する。ウイルスフレームを発信したMT102は、WB100から警告メッセージを受ける。このケースでは、ステップ1600が実行されたあと、ステップ1606が実行される。まず、自分がウイルスに汚染されているという状態数値をもち、これをセットした後、WB100から送られた当該ウイルスのワクチンプログラムを実行する(ステップ1616)。次に、これが成功したら、ウイルス駆除完了メッセージを当該WB100に報告し、ウイルス汚染状態をリセットして終了する(ステップ1608)。

【0079】次に、このウイルス駆除完了メッセージを受けるWB100の処理について図18を用いて説明する。基本ロジックは、図14で示した警告メッセージと同じ方法でウイルス駆除完了通知を近接するWBに通知する。まず、ウイルス駆除完了メッセージを受信する(ステップ1800)。次に、ウイルス保有者リストから当該MTを削除する(ステップ1802)。次に、ステップ1404からと同様の方法で警告メッセージを配布した範囲にウイルス駆除完了メッセージを配布する。このメッセージを受けたWB100の処理は、図15と同様なので詳細は省略する。ここでは、WB100が受けた持つセル内の各MT102にウイルスMTの登録解除メッセージが送られる。このメッセージを受けたMT102は、ウイルス保有者リストから通知されたMT102を削除する。

【0080】先程説明したように、MT102は、ウイルス保有者リスト上の登録されたMT102と通信する場合、ウイルス保有MTにウイルス駆除完了問い合わせを行う。図19で、この問い合わせを受けるウイルス保有MTの処理フローを説明する。まず、自分がウイルス汚染状態かどうかを確認する(ステップ1900)。その結果、対応する警告メッセージのウイルス駆除が完了していれば、問い合わせの応答として、駆除完

21

了メッセージを返送する(ステップ1902)。そして、未完了ならば、ウイルス駆除未完了メッセージを返送する(ステップ1904)。

【0081】次に、ウイルスMTへの警告メッセージの表示内容について補足説明をする。前述したようにワクチンプログラムが送られた後、ワクチンプログラムを実行するので、メッセージとして、「ウイルス退治中です、しばらくこのままお待ちください、電源切断や、移動することは控えてください」とのメッセージをワクチンプログラムが終了するまで表示しておく。

【0082】実施例7

以上の実施例は、既知のコンピュータウイルスに対抗するコンピュータネットワークシステムを示した。それは、WB100が中核となってウイルスチェック機能を行う実施例であり、主として次のようなケースに適応したものである。具体ケースとして、例えば、不特定多数がアクセスしセキュリティの管理がしっかりできないコンピュータネットワークでは既知のウイルスが潜伏している可能性がある。そのようなコンピュータネットワークにMT102が移動し、そこで情報を入手したときにウイルスに感染する可能性がある。そのご、ウイルスに感染したMT102が、セキュリティや信頼性が要求されるネットワークに戻ってきたときに、当該ネットワークの基幹部に既知のウイルスが導入するのを防ぐ場合である。

【0083】ここでは、未知のウイルスに対応するコンピュータネットワークの実施例を説明する。これは、どのようなケースに対応するかというと、例えば、信頼性の保証できないネットワークで悪質なユーザが新しいウイルスを開発しはじめた、たまたま、このようなネットワークに接続したため、未知のウイルスに感染したMT102が信頼性の要求されるネットワークに戻ってくる場合や悪質なハッカーや意図のあるユーザが直接無線ネットワークから新ウイルスを散布するケースに対応する発明である。

【0084】まず、WB100への付加機能について説明する。未知の新ウイルスは既知ウイルスの基本コードからの派生物と考えられる。そこで、WB100のウイルスチェック処理にA1手法を取り入れることにより、実施例1で示したフレーム内容とウイルスコードとの一致、不一致のみで判定するのではなく、ファジー推論により、ウイルスコードとの類似度を評価して、その評価値が或一定値以上ならば、未知のウイルスの可能性があると判断する機能を付加する。このようなWB100の処理フローを図5と図20を用いて説明する。なお、この図20は、図5からの追加・変更部を説明する。まず、ステップ502の受信フレーム待ちのあと、ステップ504の変わりに上述した方法で当該フレームにおけるウイルスの含有推定率を求め、この値によって次の3つの処理ルートに振り分ける(ステップ2000)。ま

22

ず第1のルートは、0%に近い或る値以下のケースであり、この場合は、ウイルスが含まれていないと判断して、ステップ510の中継処理に飛ぶ。第2のルートは、100%に近い或る値以上のケースであり、この場合は、ウイルスが含まれていると判定して、ステップ506の警告メッセージ作成処理に飛ぶ。第3のルートは、前記以外の値のケースであり、未知のウイルスが入っているかもしれないと判断して次のステップに進む。次のステップは、ウイルス入りのフレームかも知れないという意味の容疑メッセージを当該端末に対して送る(ステップ2002)。そして次にステップ510の中継処理から実行する。

【0085】次に、PC101の付加機能について図21を用いて説明する。まず、PCは、上記警告メッセージを受信する(ステップ2100)。次に、当該フレームを受信したAPを探し出し、それが書き込みモードでアクセスしたファイル一覧を検索し記憶する(ステップ2102)。次に、ウイルスが導入したかもしれないという警告表示をユーザにたいして提示し、合わせて、当該APの終了を促す(ステップ2104)。そして、当該APの終了を待つ(ステップ2106)。次に、ステップ2102で記憶したファイルをアクセス禁止モードにする(ステップ2108)。その後、後で詳細を説明するセキュリティサーバに対して未知のウイルスが導入した可能性のあるファイルの検査を依頼する(ステップ2110)。そして、その応答結果を受信するまで待つ(ステップ2112)。次に、その応答結果をチェックする(ステップ2114)。そして異常なならば、当該ファイルアクセス禁止モードを解除して、ユーザAPによるアクセスができるようにする(ステップ2116)。異常ありと判断されたならば、当該ファイルを削除する(ステップ2118)。

【0086】次は、セキュリティサーバを図22を用いて説明する。2200はセキュリティサーバであり、ハードウェア・ソフトウェアとも基本はPC101と同一であるため、付加機能ブロックを図で表示している。2201は、以来受け付け、結果送信ブロックであり、ここで、PC101からの検査を依頼されたファイルを受け付け、またその検査結果をPC101に対して送信する。以下の機能ブロックで実現される依頼ファイルのシミュレート実行で異常を検出しなければ、ファイル検査依頼のあったPC101に異常なしとの応答を返し、そうでなければ、異常ありとの応答を返す。2202は、依頼環境構築部であり、依頼のあったPCのゲームの動作環境を構築する機能ブロックである。2203は、依頼されたファイルのテスト実行の結果、異常が起らないか監視し、これを検出する機能ブロックである。ここには、ウイルスが原因となる異常を検出する機構、具体的には、ファイルサイズの増分チェックやメモリスキャンチェックによるウイルス寄生部の検出機能等

23

を備えている。2204は、依頼ファイルのエミュレート実行部であり、2202で設定された動作環境で、時刻タイマーのアップや当該ファイルの複数回実行をシミュレートする機能ブロックである。以上の機能ブロックを備えた計算機がセキュリティサーバである。

【0087】以上は、ウイルス検査機能をセキュリティサーバというネットワーク上の専用計算機にて実現する例を説明したが、高速のCPUや大規模なメモリを持つ事でWB100においてもその中継性能を低下させることなく実現する事ができる。

【0088】実施例8

次に、前述したセキュリティサーバ2200で異常のあったファイルから未知のウイルスを抽出し、その識別情報を各WB100に通知することで、未知のウイルスを既知の物としてWBに自動登録する機構を図23を持ちて説明する。

【0089】このとき、セキュリティサーバは2200は新規ウイルス登録メッセージを各WB100宛にマルチキャストする。図14と図15で説明したと同様な方法で代表Wbが隣接ネットの代表Wbにウイルス登録メッセージを通知する事でネットワーク全体に配布される。

【0090】一方のWBでは、新規ウイルス登録メッセージを受信する(ステップ2300)。次に、ウイルスコードシグネチャリストに前記メッセージの内容を登録する(ステップ2302)。このようにして、以後登録されたウイルスを含むフレームは、WB100でフィルタリングされる事になる。無論ここで、新規ウイルス登録メッセージに記述されたウイルスコードは、前にウイルスフレームのカプセル化手法で述べたようにWBにおけるウイルスフレームのフィルタリング例外とする。

【0091】なお、セキュリティサーバ2200が発見した未知のウイルスに対するワクテンソフトを作成し、これを新規ウイルス登録メッセージに付加する事で各WB100に配布してよい。

【0092】その他、ワクテンソフトが格納されたセキュリティサーバ2200のアドレスを新規ウイルス登録メッセージを受けたWB100に登録させておき、その後、前記メッセージによって登録されたウイルスの警告メッセージをPC101やMT102に送る。WB100は、前記PC101やMT102からの問い合わせに応じてワクテンを保有するSSのアドレスを通知する。そして、このアドレス通知を受けたPC101やMT102が当該セキュリティサーバから当該ウイルスのワクテンをロードする方法でもよい。これでPC101やMT102における未知ウイルスにたいする対応がなされる。

【0093】実施例9

前述の例では、セキュリティサーバ2200が新規ウイルス登録メッセージをマルチキャストで各WBに配布す

24

ると説明したが、隣接するWB100間で定期的にウイルスシグネチャコードリスト120の新規追加部分を教え合い、自分に足りない物が隣接WBにあればそれを取得するという方法でも配布できる。これは、ネットワークの事故や当該Wbの電源オフ等により新規ウイルス登録メッセージを受け取れなかったWb100が存在した場合に有効な方式である。この処理方法について図24で説明する。処理フロー2400は、通知処理フローである。まず、タイマを起動し一定時間に達するまで待つ(ステップ2402)。次に、テーブル120で新規に追加した物を選びだしこれを追加リストに編纂して隣接するWB100に通知する(ステップ2404)。ここで新規追加分を選び出すために、追加した物はその追加時刻を記述しておき、現在の時刻と追加時刻を比較し一定範囲内の物を選び出すようにする。2410は、登録処理の処理フローである。

【0094】まず、通知された追加リストを受取り、その内容を見て、現在テーブル120に登録されていない物が存在するかどうかをチェックする(ステップ2414)。登録すべき物があるならテーブル120に登録する(ステップ2414)。以上で処理を終了する。

【0095】以上実施例のようにならば、以下の効果がある。

【0096】1. まず、はじめに、実施例のように構成すれば、コンピュータネットワークシステムへのコンピュータウイルスの進入を防止できる。つまり、不特定多数のコンピュータが接続しウイルスが進入する可能性があるようなセキュリティ面で不安があるが、しかし、リアルタイムで有用な情報をアクセスできるようなネットワーク、例えば、インターネットと、従来から存在するセキュリティレベルの高い企業内ネットワークとをセキュリティレベルを損なうことなく接続できる。その結果、オープン化に対応したネットワークシステムを構築する事ができ、その結果、有効な情報を安全に入手できるという効果がある。

【0097】また、移動端末が普及した企業内ネットワークにおいて、移動端末が一旦企業内ネットワークから離れて、様々な情報活動を行う。例えば、他の信頼性の無いネットワークにアクセスして情報を入手したり、CD-ROM等の流通メディアをアクセスしたりである。

【0098】この後、移動端末が再度企業内ネットワークに接続されるケースで、再接続の前に、ウイルスチェックプログラムを起動し、ウイルスに感染していない事を確認しなくても、同程度のセキュリティレベルを維持する事ができる。つまり、再接続時のウイルス駆除処理オーバーヘッドを必要とせず、かつ、セキュリティレベルはそのままで、スムーズに元のネットワークにアクセスできる。また、移動端末では、ウイルスチェックプログラムを定期的に起動しなくても済むという効果もある。

25

【0099】2. また、上記のように構成すれば、ネットワークの中継装置にウイルスフィルタ機能を設けたことにより、各コンピュータにウイルスフィルタ機能を設けなくとも済む。これにより、当該ネットワークシステムにウイルスフィルタ機能を追加するためのコストを低減できる。つまり、本中継装置でウイルスに強いネットワークを構成できる。その上、各コンピュータには、ウイルスフレームを扱う処理を組み込まなくて済むため、ウイルスフレーム処理を参照して悪用しようとするユーザを未然に防止するという効果もある。また、ウイルスの侵入ターゲットとなったコンピュータで処理をしないため、安全であり、かつ、このためのオーバーヘッドをコンピュータにかけなくて済むという利点もある。

【0100】3. また、他の実施例によれば、そのネットワークの構成上理由から先に述べたウイルスフィルタ機能を備える事ができないネットワークシステムにおいて、ネットワークシステムに接続されたコンピュータは、ウイルス入りのデータを受信すると、警告メッセージが送られるため、ネットワーク上からウイルスが進入した事を当該コンピュータで認識できる。その結果、進入したウイルスに対応した処理を行う事ができるため、定期的なウイルスチェックプログラムを走らせずともよくなるという効果がある。また、ウイルス受信後、直ちに、ワクテンプログラムを走らせる事ができ、コンピュータウイルスの二次感染を防止するという効果もある。

【0101】4. また、ネットワーク監視装置にウイルス検出機能を持たせたことで、当該装置で集中的に監視することにより、それぞれのコンピュータでウイルス検出をしなくて済むので、ネットワークに接続した各コンピュータへの負担を増大させなく、ウイルスに対抗するシステムを実現できるという効果がある。

【0102】5. 警告メッセージを受けたコンピュータにその内容が表示される事で、ウイルスを受信したコンピュータのユーザは、ウイルスを送信したコンピュータを知ることができ、そこから、何をアクセスした結果ウイルスが進入する事になったか、ウイルス侵入原因の解明を行える。また、その後当該コンピュータからのアクセスを控える事により、ウイルスの進入をユーザレベルで抑止できる。ウイルスを送ったコンピュータにも警告メッセージが送られるため、知らないうちに感染していた事が分かり、その時点でワクテンプログラムを実行させる事でウイルスの駆除ができる。

【0103】6. また、ウイルスフィルタ機能を備えたネットワークシステムにおいては、ウイルス入りデータは受信できなくなる。このため、前記データを受信しようとしたAPIは、異常終了する事になる。本発明では、ネットワークの故障による異常終了とネットワークシステムのウイルスからの防衛のためによる異常終了を切り分ける事ができるという効果もある。

【0104】7. また、ある特定のネットワーク管理社

26

宛には、ウイルス入りのデータをフィルタすることなく正常に送る事で、ウイルスの解析や対抗するワクテンの開発に役立てる事ができるという効果もある。

【0105】8. また、ネットワーク上を流れるデータが圧縮されていたり、暗号化されていたりしてもウイルスのチェックができるという効果もある。

【0106】9. また、他の発明によれば、ウイルス入りのデータを送受したコンピュータに対して、当該ウイルス用のワクテンプログラムがウイルスを検出した時点で送られるため、直ちにウイルスを駆除できるという効果もある。また、コンピュータにはワクテンプログラムを保存しておく必要がないため、その分の記憶容量が多く使えるメリットもある。

【0107】10. モバイルコンピュータがウイルスを保持していた場合、それを検出したあるネットワーク監視装置が、モバイルコンピュータの移動先のネットワーク監視装置にメッセージを送る事で、ウイルスに事前にウイルス対策の準備ができる。また、メッセージの配布範囲を限定した事により、ネットワークにかかる負担を少なくするという効果もある。

【0108】11. モバイルコンピュータのウイルス駆除処理において、適切なメッセージをユーザを提示することにより、確実にウイルスの駆除を行え、また、ウイルスの拡散を防止するという効果もある。

【0109】12. その他の実施例によれば、ウイルスを保持しているコンピュータを知ることができ、ウイルスを保持しているコンピュータとの通信をしない事で、ウイルス感染の恐れを防ぐという効果がある。

【0110】13. また、モバイルコンピュータにおいては、ウイルスが検出されたエリアが分かれるので、そこエリアに移動することを避ける事でウイルスの感染を防止できる。

【0111】14. また、他の実施例によれば、ウイルス保持コンピュータをネットワーク監視装置によりウイルス保有コンピュータを一管理する事で、各コンピュータにおけるウイルス保有コンピュータの一覧を保持しなくて済むという効果がある。

【0112】15. また他の実施例によれば、新しいコンピュータウイルスを遡り検出する事ができるため、当該ネットワークで今までに存在していなかったコンピュータウイルスによる被害を食い止める事ができる。

【0113】16. また、ウイルスフィルタ機能を備えたネットワーク中継装置にウイルス推定機能を追加した事で、疑わしいデータフレームにマークを付加する事ができ、当該データを受け取ったコンピュータは前記マークをみる事で容易に疑わしいデータである事を認識できるという効果がある。

【0114】17. また、ウイルスが含まれている可能性のあるファイルをリモートにある検査専用コンピュータにその検査を依頼している最中に、その疑わしいファイ

10

20

30

40

50

27

ルのアクセスを禁じたため、もし、当該ファイルにウイルスが含まれていた場合に第3のコンピュータへ拡散することを防ぐという効果がある。

【01115】18. ウイルス検査専用コンピュータを当該ネットワークシステム内に設ける事で、システムにおける通常処理の能力を低下させることなく、コンピュータウイルスに強いネットワークシステムを構築できるメリットがある。

【01116】19. 新規ウイルスの識別情報をウイルスフィルタリング実行機器に配布する事で、以降同一のウイルスは、フィルタリングで落とされるので、コンピュータは、ウイルス検査専用コンピュータに御恩付きをもらう処理しなくても済むという効果がある。

【01117】20. ウイルスフィルタリング機能を備えたネットワーク中継機器でウイルスの識別情報を定期的に交換しあうため、当該中継機器が障害等により新しいウイルス識別情報を受信できなかった場合でも、一定時間後には、受信できることが保証されるという効果もある。

【01118】21. ウイルスチェック機能を備えたネットワーク監視装置で未知のウイルスを新規ウイルスとして検出できるようになるという効果がある。

【01119】22. 上記ネットワーク監視装置に新規ウイルスにたいするワクチンが配布されるため、新規ウイルスを検出したら、対応するワクチンプログラムを関連コンピュータに配布し、これを受信したコンピュータ上で前記の新規ウイルスの駆除ができるという効果がある。

【0120】

【発明の効果】以上の説明から明らかなように、本発明によれば、コンピュータウイルスへの耐性が強いコンピュータネットワークシステムを構築することができる。

【図面の簡単な説明】

【図1】本発明の一実施例を示すネットワーク防疫システムの概要構成図である。

【図2】本発明の一実施例を示すコンピュータウイルスフィルタリング機能を無線LANブリッジで実現したブロック図である。

【図3】図2の無線LANブリッジのハードウェア構成例を示す図である。

【図4】図2の無線LANブリッジのソフトウェア構成図である。

【図5】図2の無線LANブリッジの主要な処理のフローチャート図である。

【図6】図6(a)は、無線LANブリッジとPCとの管理プロトコルシーケンス図であり、図6(b)は、無線LANブリッジとPCとの管理プロトコルで渡される

28

メッセージの形式を示す図である。

【図7】PCにおけるセキュリティ管理プログラムの処理フローチャートである。

【図8】PC上のソフトウェア構成図である。

【図9】PCのハードウェア構成図である。

【図10】警告メッセージ通知画面の一例を示す図である。

【図11】ウイルス判定処理の処理フローチャートである。

【図12】ウイルスコードシグネチャリストの構造を示す図である。

【図13】警告メッセージのシーケンスを説明する図である。

【図14】警告メッセージ発行処理の処理フローチャートである。

【図15】警告メッセージ配布処理の処理フローチャートである。

【図16】警告メッセージ受信処理の処理フローチャートである。

【図17】ウイルス保有コンピュータとの通信を控える処理の処理フローチャートである。

【図18】ウイルス駆除完了受信処理の処理フローチャートである。

【図19】ウイルス駆除完了問い合わせの受け付け処理の処理フローチャートである。

【図20】ウイルス推定ロジックを付加したときの処理フローチャートである。

【図21】PCにおけるウイルス検査依頼処理の処理フローチャートである。

【図22】セキュリティサーバの説明図である。

【図23】新規ウイルス登録処理の処理フローチャートである。

【図24】新規ウイルス情報交換処理の処理フローチャートである。

【図25】ウイルス保有者リストの構造を示した図である。

【符号の説明】

100…無線ブリッジ、

101…パーソナルコンピュータ、

102…モバイルコンピュータ、

120…ウイルスコードシグネチャリスト、

202…ウイルスチェックブロック、

203…警告メッセージフレーム作成ブロック、

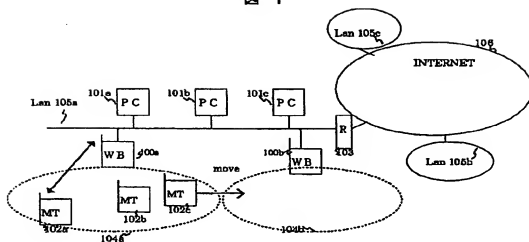
250…ウイルス保有者リスト、

600…警告メッセージ、

2200…セキュリティサーバ。

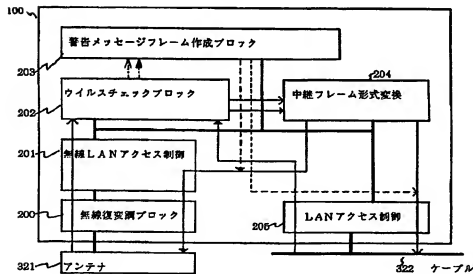
【図 1】

図 1



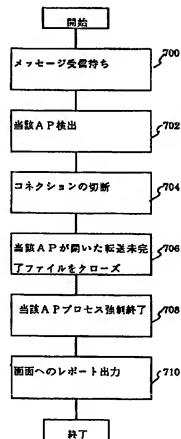
【図 2】

図 2



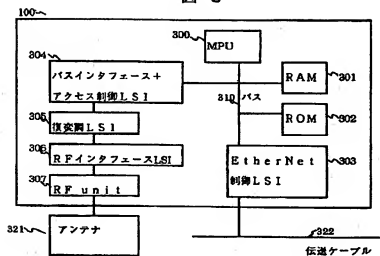
【図 7】

図 7



【図 3】

図 3



【図 1 2】

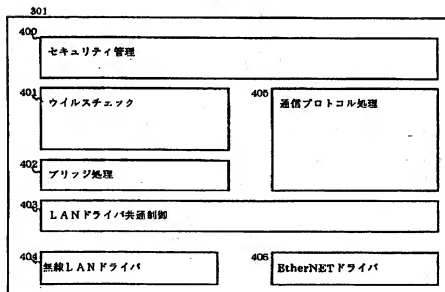
図 12

120

| ウイルスコードシグネチャリスト | |
|-----------------|-----|
| 名称 | コード |
| | |
| | |
| | |
| | |
| | |
| | |

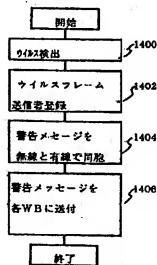
【図 4】

図 4



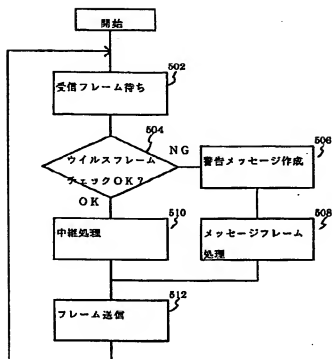
【図 1 4】

図 14



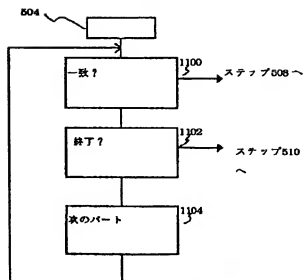
【図 5】

図 5



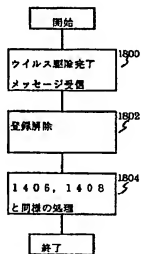
【図 11】

図 11



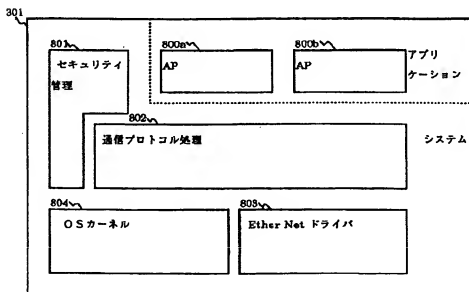
【図 18】

図 18



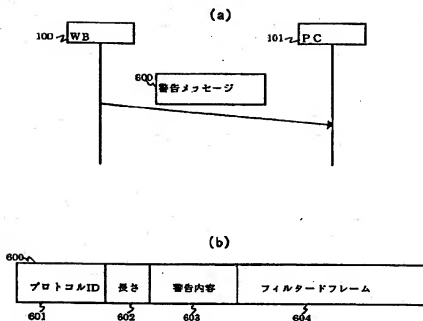
【図 8】

図 8



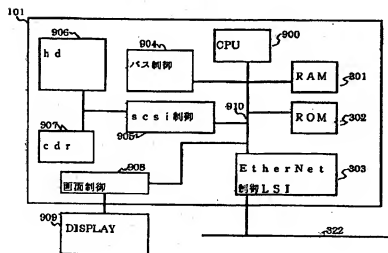
【図6】

図 6



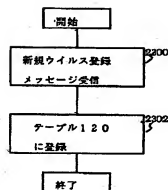
【図9】

図 9



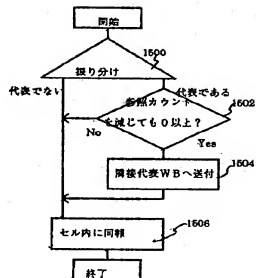
【図23】

図 23



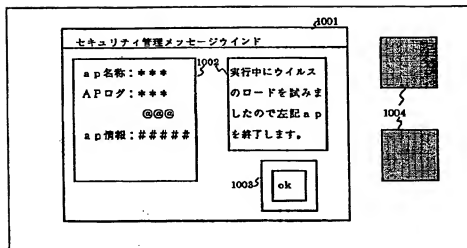
【図15】

図 15



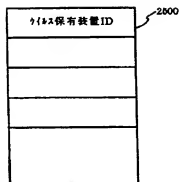
【図10】

図 10



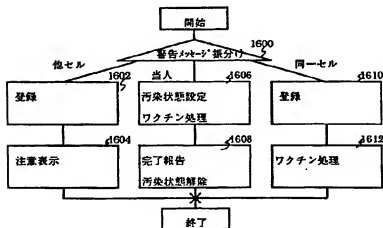
【図25】

図 25



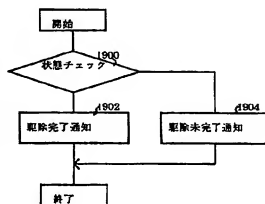
【図16】

図 16



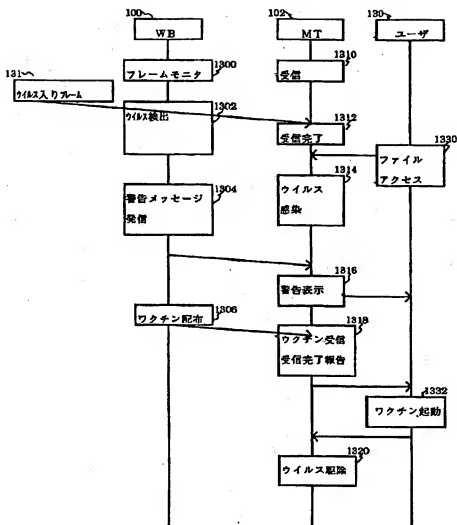
【図19】

図 19



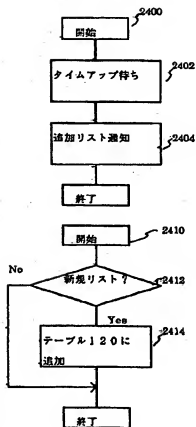
【图 13】

图 13



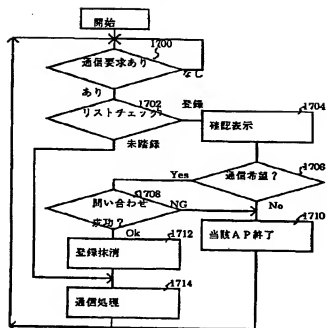
【图 2 4】

圖 24



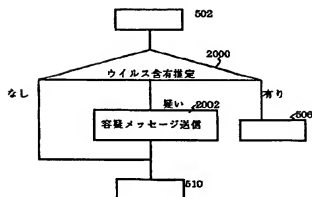
【図 17】

図 17



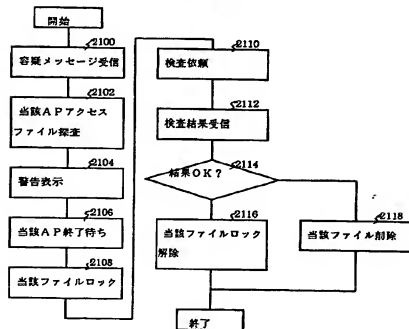
【図 20】

図 20



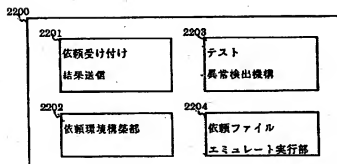
【図 21】

図 21



【図22】

図 22



THIS PAGE BLANK (USPTO)